(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－215171
（P2000－215171A）
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｅ	２Ｃ００５
Ｂ４２Ｄ　15/10	５０１	Ｂ４２Ｄ　15/10	５０１Ｌ	５Ｂ０８５
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	９Ａ００１
			６７３Ｄ	

審査請求　未請求　請求項の数13　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－18030

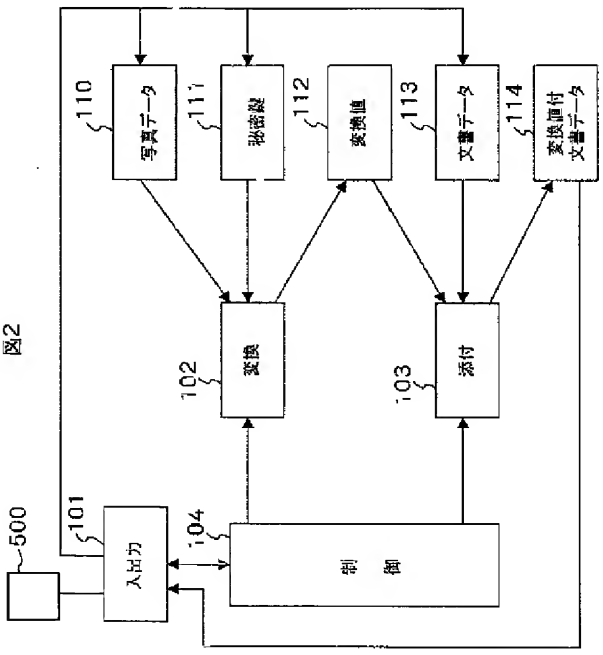
(22)出願日　平成11年１月27日(1999.1.27)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　佐々木　良一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　岩村　充
東京都練馬区中村２－14－17
(74)代理人　10008/170
弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　認証システムおよび認証方法

(57)【要約】
【課題】偽造困難な身分証明書を実現する。
【解決手段】変換部１０２は対象者の顔写真の写真データ１１０を、身分証明発行者の秘密鍵１１１で暗号化した変換値１１２を作成する。添付部１０３は、入出力部１０１を介して、変換値１１２を対象者の氏名住所などの文書データ１１３に添付した変換値付文書データを携帯可能な電子的な記録媒体５００に記録する。記憶媒体５００は対象者に発行され、認証時には、記録媒体５００に含まれる変換値を、身分証明発行者の公開鍵で復号した写真データの表す画像に写された人物と、記録媒体５００の所持者が同一人物かどうかを判定する。



【特許請求の範囲】
【請求項１】物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証システムであって、
記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段とを有する記録体作成装置と、
前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号し、前記記録体によって認証可能とされた物理的個体の特徴の値を復元する手段を有する認証用装置とを有することを特徴とする認証システム。
【請求項２】物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証システムであって、
物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を蓄積するデータベースと、記録体によって認証可能とすべき物理的個体の前記特徴値を、前記データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成する手段と、生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段とを有する記録体作成装置と、
前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号して検索情報を復元する手段と、復元された検索情報を用いて、前記記録体作成装置の前記データベースから、前記記録体によって認証可能とされた物理的個体の特徴値を検索する手段とを有する認証用装置とを有することを特徴とする認証システム。
【請求項３】請求項１または２記載の認証システムであって、
前記認証用装置は、特定の物理的個体の前記特徴値を取り込む手段と、前記前記記録体によって認証可能とされた物理的個体の特徴値とを比較し、比較結果を提示する手段を有することを特徴とする認証システム。
【請求項４】物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証方法であって、
記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成するステップと、
前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップと、
前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号し、前記記録体によって認証可能とされた物理的個体の特徴値を復元するステップと、
復元された前記記録体によって認証可能とされた物理的個体の特徴値と、前記記録体によって認証可能とされていると称される物理的個体の前記特徴値とを比較するステップとを有することを特徴とする認証方法。
【請求項５】物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証方法であって、
記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、前記データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成するステップと、
生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成するステップと、
前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップと、
前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号して検索情報を復元するステップと、
復元された検索情報を用いて、前記記録体作成装置の前記データベースから、前記記録体によって認証可能とされた物理的個体の特徴値を検索するステップと、
検索した前記記録体によって認証可能とされた物理的個体の特徴値と、前記記録体によって認証可能とされていると称される物理的個体の前記特徴値とを比較するステップとを有することを特徴とする認証方法。
【請求項６】物理的個体を認証するための情報を記録した記録体を作成する記録体作成装置であって、
記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、
前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段とを有することを特徴とする記録体作成装置。
【請求項７】物理的個体を認証するための情報を記録した記録体を作成する記録体作成装置であって、
物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を蓄積するデータベースと、
記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成する手段と、
生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成する手段と、

前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段とを有することを特徴とする記録体作成装置。
【請求項８】物理的個体を認証するための情報を記録した記録体を作成する方法であって、
記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成するステップと、
前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップとを有することを特徴とする方法。
【請求項９】物理的個体を認証するための情報を記録した記録体を作成する方法であって、
記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成するステップと、
生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成する手段と、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップとを有することを特徴とする方法。
【請求項１０】電子計算機に読み込まれ実行されるプログラムを記憶した記憶媒体であって、
前記プログラムは、前記電子計算機に、物理的個体を認証するための情報を記録した記録体を作成させるプログラムであって、かつ、前記プログラムは、記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成するステップと、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップとを前記電子計算機に実行させるプログラムであることを特徴とする記憶媒体。
【請求項１１】電子計算機に読み込まれ実行されるプログラムを記憶した記憶媒体であって、
前記プログラムは、前記電子計算機に、物理的個体を認証するための情報を記録した記録体を作成させるプログラムであって、かつ、前記プログラムは、記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成するステップと、生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成するステップと、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップとを前記電子計算機に実行させるプログラムであることを特徴とする記憶媒体。
【請求項１２】物理的個体を認証するための情報を記録した記録体であって、
記録体によって認証可能とする物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を記録した領域と、当該物理的個体について証する情報が記録された領域とを有することを特徴とする記録体。
【請求項１３】物理的個体を認証するための情報を記録した記録体であって、
データベースに格納された、記録体によって認証可能とする物理的個体の前記特徴の値を検索するための検索情報を公開鍵暗号に従った秘密鍵で暗号化した暗号情報を記録した領域と、当該物理的個体について証する情報が記録された領域とを有することを特徴とする記録体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、人物を認証するための情報が記述された身分証明書などの、何らかの物理的個体を認証するための情報が記述された記録体に関するものであり、特に、その偽造を防止する技術に関するものである。
【０００２】
【従来の技術】物理的個体を認証するための情報が記録された記録体としては、運転免許証や、パスポート、社員証などの各種身分証明書、各種鑑定書などがある。これらは、物理的個体を認証するための文字や写真による情報を、紙や紙に準じる物体に直接視認可能なように印刷や筆書などの方法により記録したものである。
【０００３】また、多くの場合、物理的個体を認証するための情報は、物理的個体を特定するための情報と、その物理的個体について証される情報よりなる。たとえば、パスポートには、物理的個体を特定するための情報として顔写真が貼付され、物理的個体について証される情報として人物の氏名、住所、生年月日、国籍などが記録される。
【０００４】物理的個体を認証するものは、記録媒体に記録された物理的個体を特定するための情報によって物理的個体を特定し、特定した物理的個体について、記録媒体に記録された物理的個体について証される情報を認証する。たとえば、パスポートであれば、空港に配置される入出国管理官などの認証者は、パスポートに貼付られた顔写真とパスポートの所持者の人相が一致する場合に、パスポートの所持者がパスポートに記録されている氏名、住所、生年月日、国籍などを持つ人間であることを認証する。
【０００５】
【発明が解決しようとする課題】さて、これら運転免許

証や、パスポート、社員証などの各種身分証明書、各種鑑定書などは、犯罪目的のために偽造の対象となることがある。たとえば、パスポートであれば、偽造パスポートは密入国や密輸や犯罪者の渡航などに使用されることがある。したがって、これら偽造を防止することは、社会的な要請である。

【０００６】これら偽造を防止するために現在まで々な工夫が成されてきているが、その度に偽造も巧妙を極め、未だ、決定的な対策が見いだされていないのが現状である。特に、正規のパスポートの顔写真の貼り換えによる偽造は、その発見が容易でないことより大きな問題となっている。

【０００７】そこで、本発明は、偽造、特に、パスポートの顔写真などの、物理的個体を特定するための情報の偽造をより効果的に防止することができる、物理的個体を認証するための情報を記録した記録体を提供することを課題とする。

【０００８】

【課題を解決するための手段】前記課題達成のために、本発明は、たとえば、物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証システムであって、記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、前記暗号情報および物理的個体について証する情報を前記記録体に記録する手段とを有する記録体作成装置と、前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号し、前記記録体によって認証可能とされた物理的個体の特徴の値を復元する手段を有する認証用装置とを有することを特徴とする認証システムを提供する。

【０００９】このような認証システムによれば、記録体によって認証可能とすべき物理的個体を特定する情報として、単なる物理的個体の写真などの物理的個体の特徴値ではなく、所定の秘密鍵で暗号化した物理的個体の特徴値を記録する。そして、認証時には、暗号化に用いた秘密鍵と対の公開鍵で復号した特徴値と、記録体によって認証されると称される物理的個体の特徴値との比較によって、物理的個体を認証する。ここで、このような公開鍵で復号した場合に偽の物理的個体の特徴値となるデータを偽造することは、対の秘密鍵を知らない限り極めて困難であり、かつ、秘密鍵を公開鍵や秘密鍵で暗号化された特徴値から導くことも極めて困難である。したがって、物理的個体を特定するための情報を偽造をより効果的に防止することができる認証用の記録体を提供することができる。

【００１０】なお、前記物理的個体は人間であって、前記個々の物理的個体を識別するために用いることのできる物理的個体の特徴は、人間の身体的特徴であってよい。また、前記物理的個体の特徴を人間の身体的特徴とした場合において、前記記録体によって認証可能とする物理的個体を写した画像を、当該記録体によって認証可能とする前記物理的個体の特徴値として用いるようにしてよい。

【００１１】

【発明の実施の形態】以下、本発明の実施形態を、物理的個体を認証するための情報を記録した記録体が、身分証明を行う記録体であるところの身分証明体である場合を例にとり説明する。

【００１２】まず、第１の実施形態について説明する。

【００１３】図１に、本第１実施形態に係る認証システムの構成を示す。

【００１４】図示するように、本認証システムは、身分証明体を発行する１または複数の発行側装置１００と、身分証明体に基づいて身分を認証する１または複数の認証側装置２００を備える。ここで、本第１実施形態に係る身分証明体は、電子データを記憶する、携帯型の電子的記録媒体であり、例えば、メモリカードやICカードや磁気カードなどの電子カードである。

【００１５】図２に示すように、発行側装置１００は、入出力部１０１と制御部１０４と変換部１０２と添付部１０３を有している。入出力部１０１は、身分証明体５００によって身分を保証される者（以下、「被保証者と呼ぶ」）の顔の画像データである写真データ１１０、身分証明体５００によって被保証者の身分を保証する者又は機関（以下、「保証者」と呼ぶ）の秘密鍵１１１、被保証者の氏名や住所や生年月日などの身分証明体５００によって保証する被保証者についての事項を記述した文書データ１１３を発行側装置１００に取り込む。また、入出力部１０１は、身分証明体５００に後述する変換値付文書データ１１４を記録する。また、変換部１０２は、写真データ１１０を秘密鍵１１１で暗号化した変換値１１２を作成する。添付部１０３は、文書データ１１３に変換値１１２を添付し、前述した変換値付文書データ１１４を作成する。制御部１０４は、入出力部１０１と変換部１０２と添付部１０３の以上の動作を制御する。

【００１６】ただし、発行側装置１００は、図３に示すように、実際には、ＣＰＵ３０１や、主記憶３０２、ハードディスク装置である外部記憶装置３０３a、他の外部記憶装置である３０３ｂ、通信制御装置３０４、キーボードやポインティングデバイスなどの入力装置３０５、表示装置などの出力装置３０６、画像データを取り込む画像入力装置３０８、身分証明体であるところの電子カードへの書き込みを行う電子カード書き込み装置３０９などを備えた、電子計算機上に構築することができる。ここで、画像入力装置３０８は、被保証者を撮影した写真から画像を取り込むものであっても、直接、被保証者を撮影し、その画像を取り込むものであってもよい。

【００１７】この場合、図２の入出力部１０１と制御部１０４と変換部１０２と添付部１０３は、ＣＰＵ３０１が主記憶３０２にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。このプログラムは、予め、外部記憶装置３０３aに記憶され、必要に応じて主記憶３０２にロードされ、ＣＰＵ３０１によって実行される。または、可搬型の記憶媒体３０７、たとえば、CD-ROMを扱う外部記憶装置３０３bもしくは通信制御装置２０４を介して、直接、必要に応じて、可搬型の記憶媒体３０７もしくはネットワークから主記憶３０２にロードされ、ＣＰＵ３０１によって実行されるか、もしくは、一旦、ハードディスク装置などの外部記憶装置３０３a上にインストールされた後、必要に応じて主記憶３０２にロードされ、ＣＰＵ３０１によって実行される。

【００１８】次に、図４に示すように、認証側装置２００は、撮影部２０１、入出力部２０２、制御部２０３、変換部２０４、比較部２０５を有する。

【００１９】入出力部２１３は、保証者の公開鍵２１１を取り込んだり、撮影部２０１を介して被保証者を自称する者の顔の画像データであるところの顔画像データ２１３を取んだり、身分証明体５００に記憶された変換値付文書データ２１０を取り込んだりする。また、入出力部２１３は、後述する比較部２０５の比較結果や、写真データ２１２の表す画像や、変換値付文書データ２１０に含まれる文書データの表示も行う。変換部２０４は、変換値付文書データ２１０に含まれている保証者の秘密鍵で暗号化された被保証者の写真データ２１２を、保証者の公開鍵で復号することにより被保証者の写真データ２１２を復元する。比較部２０５は、写真データ２１２と顔画像データ２１３をパターンマッチングの手法などにより比較し、所定程度以上両者が類似しているかどうかを比較結果として算出する。制御部２０３は、撮影部２０１、入出力部２０２、変換部２０４、比較部２０５の以上の動作を制御する。

【００２０】ただし、図５に示すように、認証側装置２００も、実際には、ＣＰＵ４０１や、主記憶４０２、ハードディスク装置である外部記憶装置４０３a、他の外部記憶装置である４０３ｂ、通信制御装置４０４、キーボードやポインティングデバイスなどの入力装置４０５、表示装置などの出力装置４０６、画像データを取り込む画像入力装置４０８、身分証明体であるところの電子カードの読み出し行う電子カード読み取り装置４０９などを備えた、電子計算機上に構築することができる。ここで、画像入力装置４０８は、被保証者を自称する者を撮影した写真から画像を取り込むものであっても、直接、被保証者を自称する者を撮影し、その画像を取り込むものであってもよい。

【００２１】この場合、図４の撮影部２０１、入出力部２０２、制御部２０３、変換部２０４、比較部２０５は、ＣＰＵ４０１が主記憶４０２にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。このプログラムは、予め、外部記憶装置３０３aに記憶され、必要に応じて主記憶４０２にロードされ、ＣＰＵ４０１によって実行される。または、可搬型の記憶媒体４０７、たとえば、CD-ROMを扱う外部記憶装置４０３bもしくは通信制御装置４０４を介して、直接、必要に応じて、可搬型の記憶媒体４０７もしくはネットワークから主記憶４０２にロードされ、ＣＰＵ４０１によって実行されるか、もしくは、一旦、ハードディスク装置などの外部記憶装置４０３a上にインストールされた後、必要に応じて主記憶４０２にロードされ、ＣＰＵ４０１によって実行される。

【００２２】以下、本第１実施形態に係る認証システムの動作について説明する。

【００２３】まず、本第１実施形態において利用する公開鍵暗号技術について簡単に説明する。

【００２４】公開鍵暗号技術は、インターネットを利用した通信などにおいて広く用いられている技術であり、この技術では、まず、ｇ（ｆ（ｎ，Ｓ），Ｖ）＝ｎ、ｆ（ｇ（ｎ，Ｖ），Ｓ）＝ｎが成立する秘密鍵Ｓ、公開鍵Ｖの組を作成する。ここでｎは任意のデータ、ｆ、ｇは所定の関数であり、上記式は、秘密鍵Ｓを用いて暗号化した任意のデータは公開鍵Vを用いて復号化することができ、また、逆に、公開鍵Vを用いて暗号化した任意のデータは秘密鍵Sで復号化できることを表している。また、ここで、公開鍵Ｖから秘密鍵Ｓを求めることは実質的に不可能となっている。

【００２５】ここで、秘密鍵Ｓ、公開鍵Ｖを作成したならば、作成者は公開鍵Ｖを、相手方に渡し、秘密鍵Ｓは作成者が秘密に保持する。

【００２６】そして、相手方が鍵の作成者にデータを送る場合、データを公開鍵Ｖで暗号化したものを鍵の作成者に渡す。そして、データを受け取った鍵の作成者は、データを秘密鍵Ｓを用いて復号化する。また、その逆の処理も可能である。つまり、鍵の作成者が、相手方にデータを送る場合には、データを秘密鍵Sで暗号化したものを相手方に渡す。そして、データを受け取った相手方は、データを公開鍵Ｖを用いて復号化する。

【００２７】ただし、実用上、安全を確保できる長さの秘密鍵を用いた暗号化や、公開鍵を用いた復号化の処理には時間を要するため、一般的には、相手方（あるいは鍵の作成者）が、鍵の作成者（あるいは相手方）にデータを送る場合には、データを一時鍵で暗号化したものと、この一時鍵を公開鍵Ｖ（あるいは秘密鍵S）で暗号化したものを鍵の作成者（あるいは相手方）に渡し、データを受け取った鍵の作成者（あるいは相手方）は、一時鍵を秘密鍵S（あるいは公開鍵Ｖ）を用いて復号化し、この一時鍵を用いてデータを復号するというように２段階の暗号化が行われている。

【００２８】また、このようなデータの暗号化の技術と共に、鍵の保持者がデータの特徴値を秘密鍵で暗号化したものを、暗号化したデータに添付し送ることにより、データを受け取ったものが、公開鍵で復号した特徴値と受け取ったデータの実際の特徴値の比較によって、データの真正性を認証可能とする、電子署名として知られる技術が用いられることが多い。この場合、データの特徴値としては一方向ハッシュ関数によるデータの評価値などの一方向関数による評価値が通常用いられる。一方向関数は、実質上、データから関数で評価した評価値を算出可能であるが、評価値から元のデータを算出することは実質的に実用上不可能である性質をもつ。

【００２９】以上、公開鍵暗号について説明した。

【００３０】次に、発行側装置１００の動作について説明する。

【００３１】図６に、発行側装置１００の制御部１０４が行う処理の手順を、図７にその処理のようすを示す。ただし、図７は、本処理の理解を容易ならしめるために、データの構成を模式的に示したものである。

【００３２】ここでは、予め、保証者の秘密鍵１１１が入出力部１０１を介して発行側装置１００内に取り込まれ、記憶されているものとする。

【００３３】さて、図示するように、ある被保証者の身分保証体５００を発行する場合、制御部１０４は、まず、入出力部１０１を制御し、被保証者の写真データ１１０と被保証者の氏名や住所や生年月日などを記述した文書データ１１３を取り込む（ステップ６０１）。

【００３４】次に、変換部１０２を制御し、図７に示すように、前述した公開鍵暗号技術に従って写真データ１１０を秘密鍵１１１で暗号化した変換値１１２を作成させる（ステップ６０２）。そして、最後に、添付部１０３を制御し、文書データ１１３に変換値１１２を添付した変換値付文書データ１１４を作成し、入出力部１０１を介して、身分保証体５００に書き込む（ステップ６０３）。

【００３５】さて、このようにして変換値付文書データ１１４が記録された身分保証体５００は、被保証者に渡され、被保証者によって携帯され、被保証者の身元の認証が必要なときに、被保証者によって提示される。

【００３６】次に、認証側装置２００の動作について説明する。

【００３７】図８に、認証側装置２００の制御部２０３が行う処理の手順を、図９にその処理のようすを示す。ただし、図９は、本処理の理解を容易ならしめるために、データの構成を模式的に示したものである。

【００３８】ここでは、予め、保証者の秘密鍵１１１が入出力部２０２を介して認証側装置２００内に取り込まれ、記憶されているものとする。

【００３９】図示するように、被保証者を自称するものから、その者が携帯する身分保証体５００の提示を受けると、認証側装置２００の制御部２０３は、まず、入出力部２０２を介して身分保証体５００から、変換値付文書データ２１０を取り込む（ステップ８０１）。そして、変換部２０４を制御し、保証者の公開鍵８０２で、変換値付文書データ２１０に含まれている保証者の秘密鍵で暗号化された被保証者の写真データ２１２を、前述した公開鍵暗号技術に従って保証者の公開鍵で復号することにより被保証者の写真データ２１２を復元させる（ステップ８０２）。

【００４０】次に、撮影部２０１、入出力部２０２を制御し、被保証者を自称する者の顔の画像を顔画像データ２１３として取り込む（ステップ８０３）。そして、比較部２０５を制御し、顔画像データ２１３と復号した写真データ２１２とをパターンマッチングの手法などにより比較し、所定程度以上両者が類似しているかどうかを比較結果として算出し、入出力部２０２を介して、比較結果を、復号した写真データ２１２が表す画像や変換値付文書データ２１０に含まれる文書データが示す文書と共に表示する（ステップ８０４）。ここで、顔画像データ２１３と復号した写真データ２１２と所定程度以上両者が類似している場合に、比較結果は、この被保証者を自称している者が確かに被保証者であって、身分保証体５００が確かに、この被保証者に対して発行されたものであることが認証された旨を示すことになる。

【００４１】以上、本発明の第１の実施形態について説明した。以上のように、本第１実施形態によれば、被保証者を特定する情報として、単なる被保証者の写真データではなく、保証者の秘密鍵で暗号化した被保証者の写真データを身分保証体に記録し、保証者の公開鍵で復号した写真データと被保証者を自称する者の顔との比較によって、被保証者を認証する。ここで、このような保証者の公開鍵で復号した場合に不正者の写真データとなるデータを偽造することは、保証者の秘密鍵を知らない限り極めて困難であり、かつ、保証者の秘密鍵を公開鍵や秘密鍵で暗号化された写真データから導くことも極めて困難である。したがって、本第１実施形態によれば、被保証者を特定するための情報を偽造をより効果的に防止することができる身分保証体を提供することができる。

【００４２】なお、以上の実施形態では、発行側装置１００において、被保証者の写真データだけを保証者の秘密鍵を用いて暗号化したが、被保証者の氏名や従者や生年月日などの身分保証体が保証する被保証者についての事項を記述した文書データも保証者の秘密鍵を用いて暗号化して身分保証体に記録するようにし、認証側装置２００において保証者の公開鍵で文書データを復号して利用するようにしてもよい。このようにすることにより、身分保証体が保証する被保証者についての事項についても、写真データと同様に、より効果的に偽造を防止することができるようになる。

【００４３】また、以上の実施形態では、認証側装置２

００において、被保証者を自称する者の顔画像データと、身分保証体に記録された保証者の秘密鍵によって暗号化された写真データを復号した画像を比較し、比較結果を表示したが、この比較は行わないようにしてもよい。すなわち、認証側装置２００は、身分保証体に記録された保証者の秘密鍵によって暗号化された写真データを復号した画像と、身分保証体に記録された文書データの表示のみを行い、認証側装置２００を利用する認証者が、表示された画像と、被保証者を自称する者とを見比べ、被保証者を自称する者が、復号した写真データが表す画像に写された人物と同一人物であるかどうかを判断するようにしてもよい。

【００４４】また、以上の実施形態において、身分保証体には保証者の秘密鍵によって暗号化された写真データのみ記録し、被保証者の氏名や従者や生年月日などの身分保証体が保証する被保証者についての事項は身分保証体と分離不可能な形態で、直接視認可能なように記録するようにしてもよい。例えば、身分保証体である電子カードの表面に偽造が困難な形態で文字を印刷やエッチングなどの手法により記録するようにしてもよい。

【００４５】以下、本発明の第２の実施形態について説明する。

【００４６】図１０に本第２実施形態に係る認証システムの構成を示す。

【００４７】図示するように、本第２実施形態に係る認証システムはネットワーク６０００を介して接続される、１以上のセンタ装置１０００と、１以上の認証側装置２０００を有する。

【００４８】ここで、本第２実施形態に係る身分証明体は、印刷などの直接視認可能な形態によって文字や図形などが記録される記録媒体であり、例えば、紙やプラスチックや金属のカードである。

【００４９】さて、図１１に示すようにセンタ装置１０００は、入出力部１００１と制御部１００２とデータベース管理部１００３と変換部１００４と添付部１００５とを有している。入出力部１００１は、被保証者の顔の画像データである写真データ１００６、保証者の秘密鍵１００９、被保証者の氏名や住所や生年月日などの身分証明体５００によって保証する被保証者についての事項を記述した文書データ１１１１を取り込む。また、入出力部１００１は、身分証明体５００に後述する変換値付文書データ１１１２を印刷によって記録する。

【００５０】また、データベース管理部１００３は、写真データのデータベース１００７を管理しており、入出力部１００１が取り込んだ写真データ１００６に登録番号１００８を与えた上でデータベース１００７に登録する。ここで登録番号１００８には、写真データ１００６を登録したセンタ装置１０００を識別するための番号を含めるようにする変換部１００４は、写真データ１００６の登録番号１００８を秘密鍵１００９で暗号化した変換値１０１０を作成する。添付部１００５は、文書データ１１１１に、変換値１０１０をバーコードによって表した図形を挿入し、前述した変換値付文書データ１１１２を作成する。

【００５１】ここで、入出力部１００１はネットワーク６０００を介して認証側装置２０００から送られた、登録番号を伴う検索要求を取り込みデータベース管理部１００３に送る。データベース管理部１００３は、検索要求に伴う登録番号の写真データをデータベース１００７から検索し、入出力部１００１に送る。入出力部１００１は、送られた写真データを、ネットワーク６０００を介して検索要求を発行した認証側装置２０００に送信する。

【００５２】制御部１００２は、入出力部１００１とデータベース管理部１００３と変換部１００４と添付部１００５の以上の動作を制御する。

【００５３】ただし、センタ装置１０００は、図１２に示すように、実際には、ＣＰＵ３００１や、主記憶３００２、ハードディスク装置である外部記憶装置３００３a、他の外部記憶装置である３００３ｂ、ネットワーク６０００に接続する通信制御装置３００４、キーボードやポインティングデバイスなどの入力装置３００５、表示装置などの出力装置３００６、画像データを取り込む画像入力装置３００８、身分証明体であるところのカード５０００への印刷を行う印刷システム３００９などを備えた、電子計算機上に構築することができる。ここで、画像入力装置３００８は、被保証者を撮影した写真から画像を取り込むものであっても、直接、被保証者を撮影し、その画像を取り込むものであってもよい。

【００５４】この場合、図１１の入出力部１００１と制御部１００２とデータベース管理部１００３と変換部１００４と添付部１００５とは、ＣＰＵ３００１が主記憶３００２にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。このプログラムは、予め、外部記憶装置３００３aに記憶され、必要に応じて主記憶３００２にロードされ、ＣＰＵ３００１によって実行される。または、可搬型の記憶媒体３００７、たとえば、CD-ROMを扱う外部記憶装置３００３bもしくは通信制御装置３００４を介して、直接、必要に応じて、可搬型の記憶媒体３００７もしくはネットワークから主記憶３００２にロードされ、ＣＰＵ３００１によって実行されるか、もしくは、一旦、ハードディスク装置などの外部記憶装置３００３a上にインストールされた後、必要に応じて主記憶３００２にロードされ、ＣＰＵ３００１によって実行される。

【００５５】次に、図１３に示すように、認証側装置２０００は、入出力部２００１、制御部２００２、変換部２００３、リモート検索部２００４を有する。

【００５６】入出力部２００１は、保証者の公開鍵２００６を取り込んだり、身分証明体５０００に印刷された

バーコードが表す数値を変換値２００５として取り込んだりする。また、入出力部２００１は、リモート検索部２００４が発行する検索要求をネットワーク６０００を介してセンタ装置１０００に送信すると共に、検索要求の応答として、センタ側装置１０００から送られた写真データをリモート検索部２００４に渡す。また、入出力部２００１は、リモート検索部２００４が検索した写真データの表す画像の表示も行う。

【００５７】変換部２００３は、変換値２００５を、保証者の公開鍵で復号することにより写真データの登録番号２００７を復号する。リモート検索部２００４は、復号された登録番号を伴う検索要求を入出力部２００１を介して、登録番号に含まれる番号より特定されるセンタ装置１０００に発行することにより、センタ装置１０００のデータベース１００７から、この登録番号の写真データを入手し、入手した写真データを表示のために入出力部２００１に渡す。

【００５８】制御部２００２は、入出力部２００１、変換部２００３、リモート検索部２００４の以上の動作を制御する。

【００５９】ただし、図１４に示すように、認証側装置２０００も、実際には、ＣＰＵ４００１や、主記憶４００２、ハードディスク装置である外部記憶装置４００３a、他の外部記憶装置である４００３ｂ、ネットワーク６０００に接続する通信制御装置４００４、キーボードやポインティングデバイスなどの入力装置４００５、表示装置などの出力装置４００６、身分証明体であるところのカード５０００に印刷されたバーコードを読み取るバーコード読み取り装置４００９などを備えた、電子計算機上に構築することができる。

【００６０】この場合、図１３の入出力部２００１、制御部２００２、変換部２００３、リモート検索部２００４とは、ＣＰＵ４００１が主記憶４００２にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。このプログラムは、予め、外部記憶装置４００３aに記憶され、必要に応じて主記憶４００２にロードされ、ＣＰＵ４００１によって実行される。または、可搬型の記憶媒体４００７、たとえば、CD-ROMを扱う外部記憶装置４００３bもしくは通信制御装置４００４を介して、直接、必要に応じて、可搬型の記憶媒体４００７もしくはネットワークから主記憶４００２にロードされ、ＣＰＵ４００１によって実行されるか、もしくは、一旦、ハードディスク装置などの外部記憶装置４００３a上にインストールされた後、必要に応じて主記憶４００２にロードされ、ＣＰＵ４００１によって実行される。

【００６１】以下、本第２実施形態に係る認証システムの動作について説明する。

【００６２】まず、センタ装置１０００の動作について説明する。

【００６３】図１５に、センタ装置１０００の制御部１００２が行う処理の手順を、図１６にその処理のようすを示す。

【００６４】ここでは、予め、保証者の秘密鍵１００９が入出力部１００１を介してセンタ装置１０００内に取り込まれ、記憶されているものとする。

【００６５】さて、図示するように、ある被保証者の身分保証体５０００を発行する場合、制御部１００２は、まず、入出力部１００１を制御し、被保証者の写真データ１００６と被保証者の氏名や住所や生年月日などを記述した文書データ１０１１を取り込む（ステップ１５０１）。

【００６６】次に、データベース管理部１００３を制御し、図１６に示すように、取り込んだ写真データ１００６に、自センタ装置を識別するための番号を含めた登録番号を与え、登録番号と共に、データベース１００７に登録する（ステップ１５０２）。

【００６７】そして、変換部１００４を制御し、前述した公開鍵暗号技術に従って写真データ１００６をデータベース１００７に登録した登録番号を、秘密鍵１００９で暗号化し変換値１１２を作成させる（ステップ１５０３）。そして、最後に、添付部１００５を制御し、文書データ１０１１が表す文書に変換値１１２をバーコード化した図形を挿入した文書を表す変換値付文書データ１０１２を作成し、入出力部１００１を介して、変換値付文書データ１０１２の表す文書を身分保証体５００に印刷する（ステップ１５０４）。

【００６８】さて、このようにして変換値付文書が記録された身分保証体５０００は、被保証者に渡され、被保証者によって携帯され、被保証者の身元の認証が必要なときに、被保証者によって提示される。

【００６９】また、制御部１００２は、前述したように、入出力部１００１がネットワーク６０００を介して認証側装置２０００から送られた、登録番号を伴う検索要求を受け取った場合に、データベース管理部１００３を制御し、検索要求に伴う登録番号の写真データをデータベース１００７から検索させ、入出力部１００１に検索された写真データを、ネットワーク６０００を介して検索要求を発行した認証側装置２０００に送信させる。

【００７０】次に、認証側装置２０００の動作について説明する。

【００７１】図１７に認証側装置２０００の制御部２００２が行う処理の手順を、図１８にその処理のようすを示す。

【００７２】ここでは、予め、保証者の公開鍵２００６が入出力部２００１を介して認証側装置２０００内に取り込まれ、記憶されているものとする。

【００７３】図示するように、被保証者を自称するものから、その者が携帯する身分保証体５０００の提示を受けると、認証側装置２０００の制御部２０２は、まず、

入出力部２００１を介して身分保証体５０００に印刷されたバーコードを読み取り、これを数値に変換し、変換値２００５とする（ステップ１００７）。

【００７４】次に、変換部２００３を制御し、変換値２００５を、保証者の公開鍵２００６で、前述した公開鍵暗号技術に従って復号することにより登録番号２００７を復元させる（ステップ１７０２）。そして、リモート検索部２００４を制御し、入出力部２００１を介して、復元された登録番号２００７を伴う検索要求を、登録番号２００７に含まれる番号で特定されるセンタ装置１０００に発行させ、この登録番号２００７でセンタ装置１０００のデータベースに登録された写真データを入手させ（ステップ１７０３）、入手した写真データが表す画像を入出力部２００１において表示させる（ステップ１７０４）。

【００７５】認証装置２０００を利用する認証者は、この表示された画像と、被保証者を自称する者とを見比べ、被保証者を自称する者が、復号した写真データが表す画像に写された人物と同一人物であるかどうかを判断する。

【００７６】以上、本発明の第２の実施形態について説明した。本第２実施形態によれば、写真データを暗号化したものに換えて、写真データの登録番号を暗号化したものを身分保証体に記録するので、前記第１実施形態に効果に加え、身分保証体に記録する情報量が少なくて済むという効果がある。このため、バーコードなどの印刷などの手法によって、紙などの非電子的な記録媒体にも、被保証者を特定する情報を記録することができる。また、登録番号より認証装置２０００において、この登録番号の写真データを登録しているセンタ装置１０００を識別可能としているので、複数のセンタ装置１０００を設けるなど、柔軟な運用が可能となる。

【００７７】なお、以上の第２実施形態では、写真データの登録番号を暗号化したものをバーコードとして身分証明体に記録したが、これは写真データの登録番号を暗号化したものを直接数値によって身分証明体に記録するようにしてもよい。また、身分証明体を電子的な記録媒体として、写真データの登録番号を暗号化したものを電子的に記録するようにしてもよい。

【００７８】また、本第２実施形態においても前記第１実施形態と同様に、認証側装置２０００において、被保証者を自称する者の顔画像データを取り込みと、身分保証体に記録された保証者の秘密鍵によって暗号化された登録番号によって検索した写真データとを比較し、比較結果を表示するようにしてもよい。

【００７９】以上、本発明の実施形態について説明した。

【００８０】なお、以上の実施形態では、被保証者の写真データを被保証者を特定するための情報とし、その暗号値もしくはその登録番号の暗号値を身分証明体に記録したが、写真データに代えてもしくは写真データと組み合わせて、被保証者の指紋、声紋、虹彩パターン、網膜パターン、身長値、体重値、遺伝子パターン、血液情報などの他の、被保証者を特徴づける情報を単独でもしくは組み合わせて用い、その暗号値もしくはその登録番号の暗号値を身分証明体に記録するようにしてもよい。

【００８１】

【発明の効果】以上のように、本発明によれば、偽造、特に、パスポートの顔写真などの、物理的個体を特定するための情報の偽造をより効果的に防止することができる、物理的個体を認証するための情報を記録した記録体を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係る認証システムの構成を示すブロック図である。

【図２】本発明の第１実施形態に係る発行側装置の構成を示すブロック図である。

【図３】本発明の第１実施形態に係る発行側装置のハードウエア構成例を示すブロック図である。

【図４】本発明の第１実施形態に係る認証側装置の構成を示すブロック図である。

【図５】本発明の第１実施形態に係る認証側装置のハードウエア構成例を示すブロック図である。

【図６】本発明の第１実施形態に係る発行側装置の行う処理の手順を示すフローチャートである。

【図７】本発明の第１実施形態に係る発行側装置の行う処理のようすを示した図である。

【図８】本発明の第１実施形態に係る認証側装置の行う処理の手順を示すフローチャートである。

【図９】本発明の第１実施形態に係る認証側装置の行う処理のようすを示した図である。

【図１０】本発明の第２実施形態に係る認証システムの構成を示すブロック図である。

【図１１】本発明の第２実施形態に係るセンタ装置の構成を示すブロック図である。

【図１２】本発明の第２実施形態に係るセンタ装置のハードウエア構成例を示すブロック図である。

【図１３】本発明の第２実施形態に係る認証側装置の構成を示すブロック図である。

【図１４】本発明の第２実施形態に係る認証側装置のハードウエア構成例を示すブロック図である。

【図１５】本発明の第２実施形態に係るセンタ装置の行う処理の手順を示すフローチャートである。

【図１６】本発明の第２実施形態に係るセンタ装置の行う処理のようすを示した図である。

【図１７】本発明の第２実施形態に係る認証側装置の行う処理の手順を示すフローチャートである。

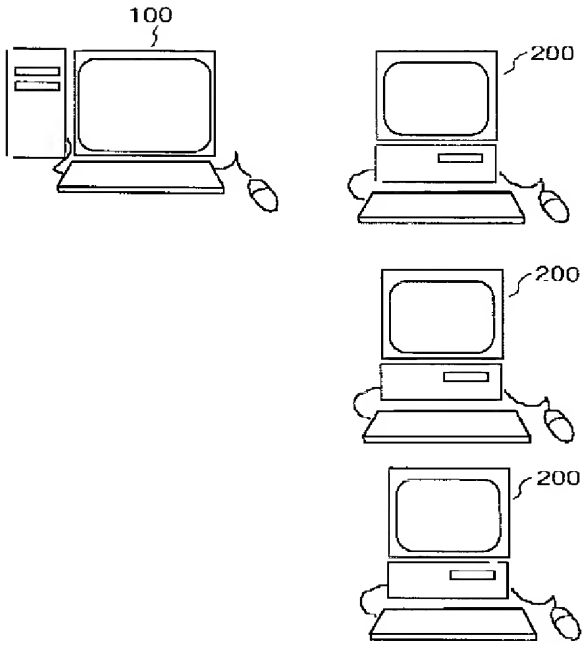
【図１８】本発明の第２実施形態に係る認証側装置の行う処理のようすを示した図である。

【符号の説明】

１００　発行側装置、１０１　入出力部、１０４　制御部、１０２　変換部、１０３　添付部、２００　認証側装置、２０１　撮影部、２０２　入出力部、２０３　制御部、２０４　変換部、２０５　比較部、５００　身分証明体、１０００センタ装置、１００１　入出力部、１００２　制御部、１００３　データベース管理部、１００４　変換部、１００５　添付部、２０００　認証側装置、２００１　入出力部、２００２　制御部、２００３　変換部、２００４　リモート検索部、５０００　身分証明体、６０００　ネットワーク

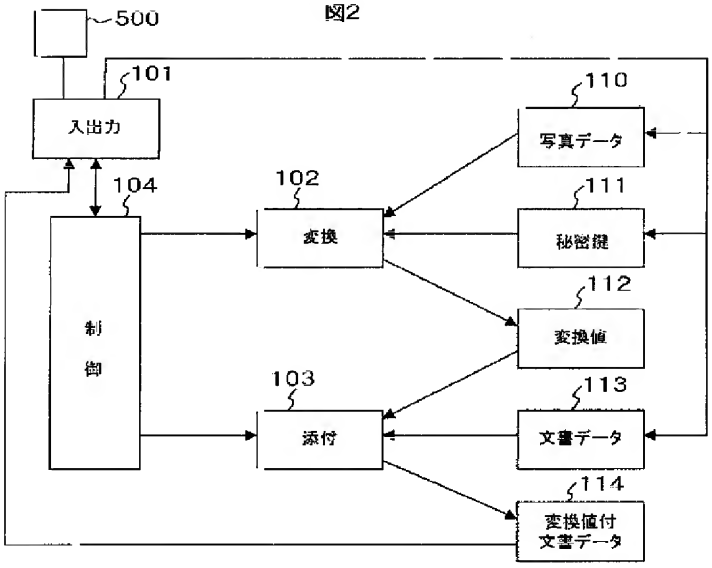
【図１】

図1



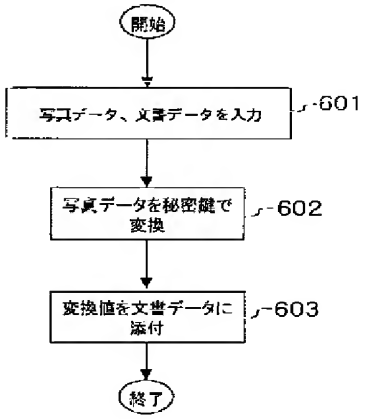
【図２】

図2



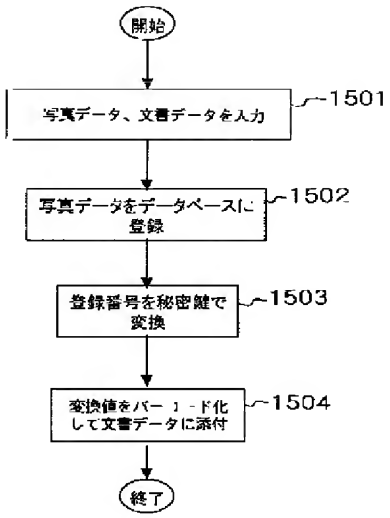
【図６】

図6



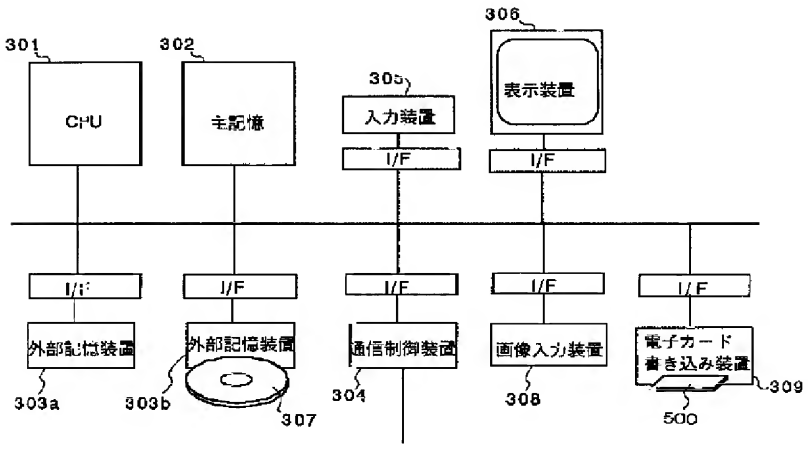
【図１５】

図15



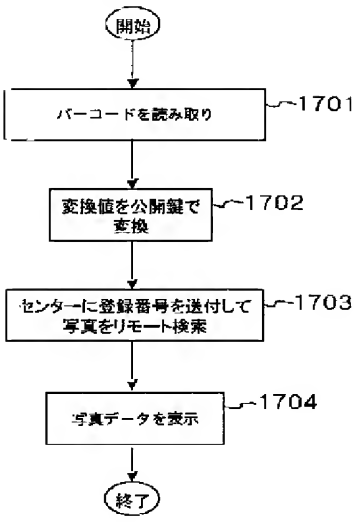
【図３】

図3



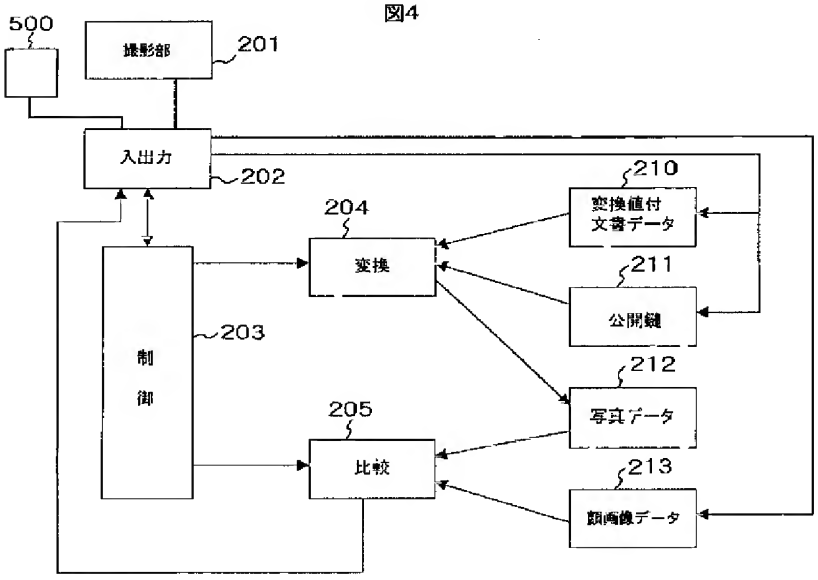
【図１７】

図17



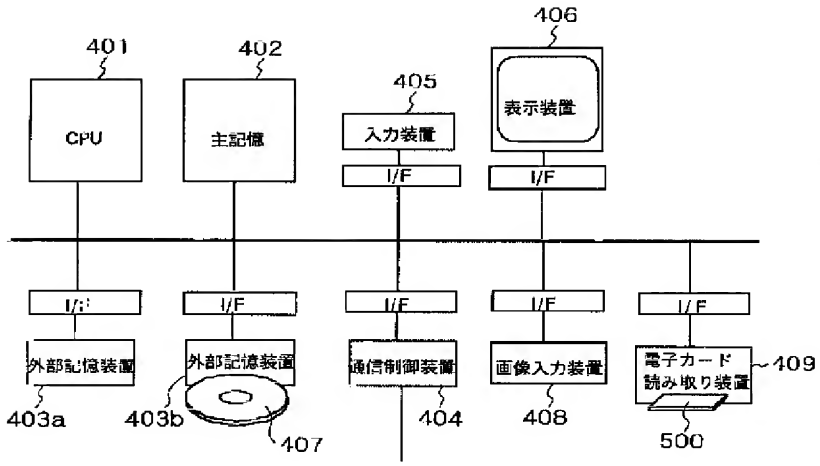
【図４】

図4



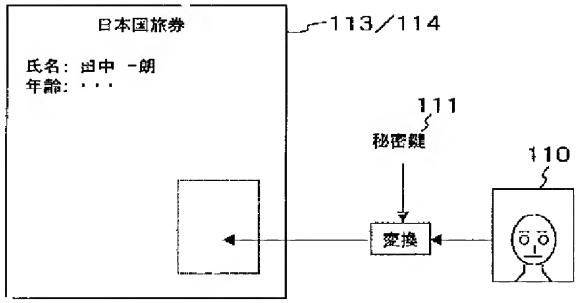
【図5】

図5



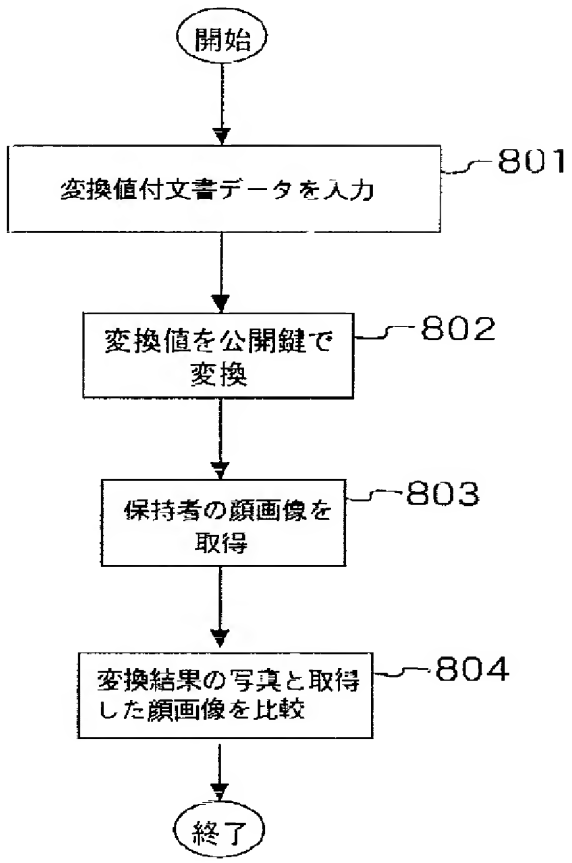
【図7】

図7



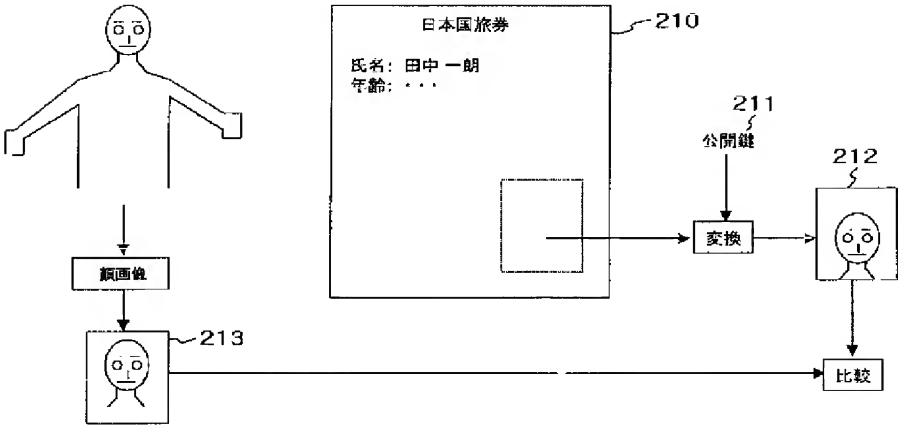
【図8】

図8



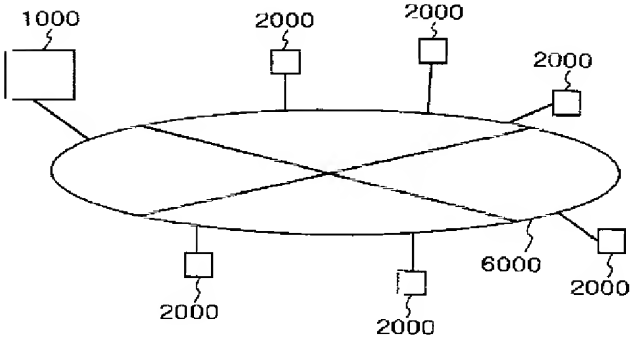
【図9】

図9



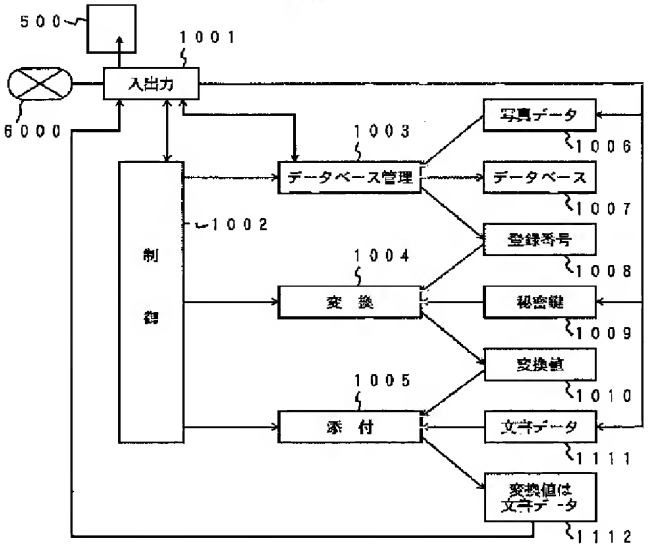
【図10】

図10



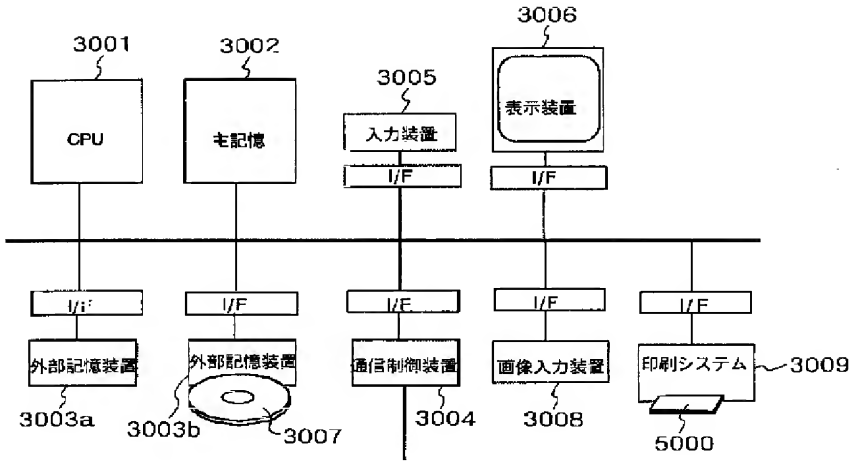
【図11】

図11



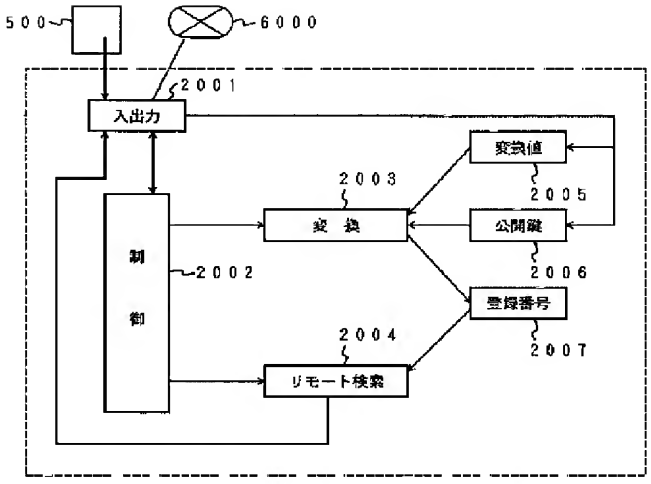
【図12】

図12



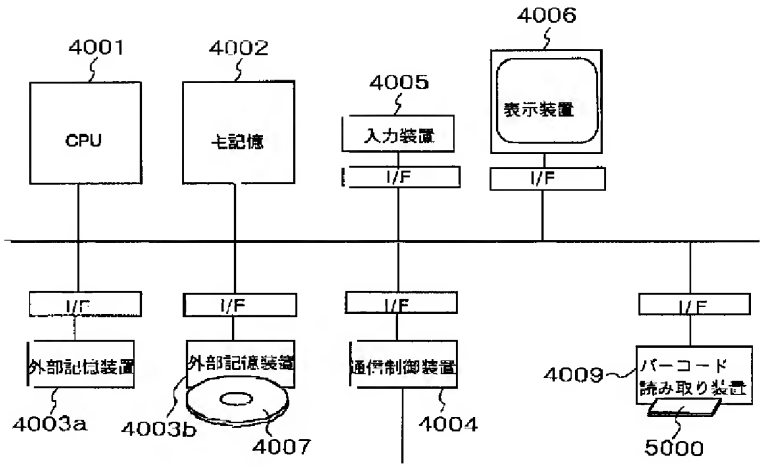
【図13】

図13



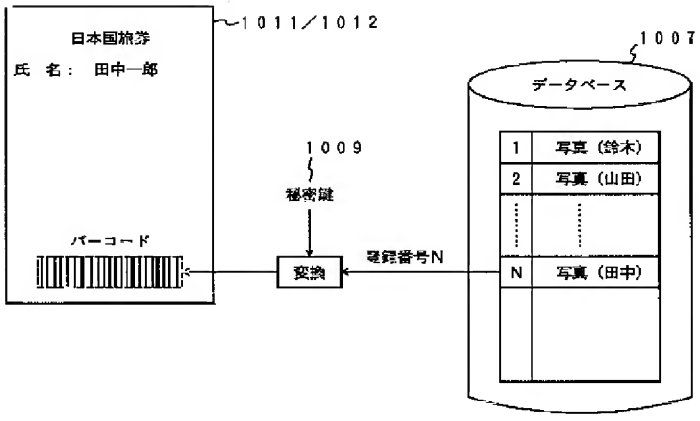
【図14】

図14



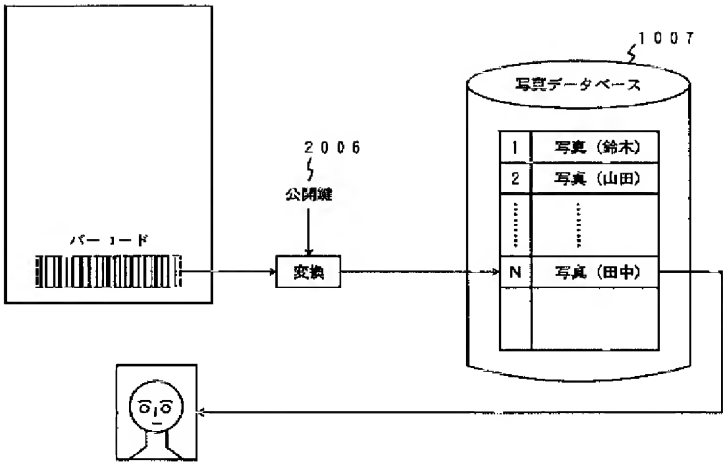
【図16】

図16



【図１８】

図18



フロントページの続き

Ｆターム(参考)　2C005 HA01 HB02 JA01 JA15 JA26
JB02 JB06 JB33 JB40 LA33
LB32 LB34
5B085 AE12 AE13 AE23 AE25 AE29
5J104 AA07 AA13 KA01 KA05 NA38
PA14
9A001 BB03 BB04 DD13 EE03 FF03
HH21 HH34 JJ01 KK42 LL03